WHAT IS CLAIMED IS:

1. A device, comprising:

a removable digital memory including a port at which digital information stored on said memory can be accessed;

a memory for storing first conditional access data and at least one content encryption key;

a second port for receiving user certificate data and a first key of a key pair contained in an access card; and

a processor responsive to the user certificate data received on said second port for authenticating the received certificate data based on the first conditional access data stored in said memory, the processor, upon said authentication, encrypting information stored in said removable digital memory using the at least one content encryption key, to thereby provide encrypted information in said removable digital memory, the processor operable for encrypting said content encryption key using said first encryption key received on said second port and outputting said encrypted content encryption key to enable access of said encrypted information stored on said removable digital memory by an external device.

2. A device according to claim 1, further comprising means for establishing that said access card is not expired.

3. A device according to claim 2, wherein said means for establishing that said access card is not expired is performed by comparing the current time with a timestamp in said received user certificate data.

4. A device according to claim 1, wherein said first key is a public key of a public/private key pair.

5. A device according to claim 1, wherein said access card is inserted into a slot of said device.

6. An access card for enabling secure accessing of digital information stored on a removable memory, the access card comprising:

a memory having stored therein a first conditional access certificate and a second conditional access certificate;

means for authenticating first and second conditional access certificates with respective first and second certificate data stored on respective destination and source devices;

said memory, following authentication of said card with a destination device, being updated to store a public key of a public/private key pair stored in said destination device; and

a processor operable for, upon authentication of said card with a source device, controlling transmission of said public key to said source device, wherein, in response thereto, said memory being updated to store encrypted data comprising a first key encrypted using said public key, said first key also being used to encrypt information on said removable memory at said source device, whereby communication of said encrypted data to said destination device enables decryption of said data using said private key to recover said first key, to thereby decrypt encrypted information in said removable memory.

7. An access card according to claim 6, further comprising an electronic time stamp.

8. A digital information destination device comprising:

a digital information input port;

a digital information decoder coupled to said digital information input port for decoding digital information encoded with a content encoding key, when said content encoding key is available, to thereby produce unencoded digital information;

memory preloaded with at least a second stored User Certificate (A) and mutually corresponding private and public encryption keys associated with said destination device;

a content encoding key decryptor for decrypting said content encoding key with a content encoding key encryption key;

an access card reader for reading an access card, where said access card includes authentication means and a memory which, prior to a first insertion in said destination device, includes at least a second Conditional Access Certificate (A)

and a first User Certificate (B) and which, after said first insertion, includes at least said public portion of said private and public encryption keys and which, prior to a subsequent insertion in said destination device, is inserted into a source device and updated to include a content encoding key encrypted with said key encryption key, whereby said destination device, following said subsequent insertion of said access card, has the key encryption key and can decrypt said content encoding key and, using said content encoding key, decode said digital information encoded with said content encoding key.

9. A method for securely transferring information from a source device to an external device, the source device having a removable digital memory containing information accessible to the source device, the information contained in said digital memory intended to be protected from unauthorized access, the method comprising:

receiving at the source device user certificate data from an access device and comparing the user certificate data with a first Conditional Access Certificate (B) stored in memory of said source device for authenticating the certificate data;

accessing said information stored in said removable digital memory and encrypting said information stored in said removable digital memory using at least one content encryption key stored in said source device, upon authentication of said certificate data;

receiving at the source device a public key from the access device and encrypting said at least one content encryption key using said public key; and

transmitting said encrypted content encryption key to enable access of said encrypted information stored on said removable digital memory by an external device communicable with said access device.

10. A method for securely porting digital information from a source device to a destination device comprising:

providing a source device having a removable digital memory and including a first Conditional Access Certificate

(B);

providing a destination device having a second stored User Certificate (A) and also including mutually corresponding private and public encryption keys associated with said destination device;

providing an access card capable of use with both said source device and said destination device, said access card including a second Conditional Access Certificate (A) and a first User Certificate (B) stored therein;

placing said access card in said access card port of said destination device a first time;

after said placing of said access card in said destination device a first time, accessing said second User Certificate certificate (A) from said destination device, and, within said access card, authenticating said second User Certificate (A) from said destination device with said second Conditional Access Certificate (A) to determine if said public encryption key should be read from said destination device and stored in said access card;

if said public encryption key of said destination device should be written to said access card, writing said public encryption key from said destination device to said access card;

removing said access card from said destination device after said writing of said public encryption key;

inserting said access card into said source device, and authenticating said first User Certificate (B) with said first Conditional Access Certificate (B) to determine if said access card is valid;

if said access card is deemed to be valid by said source device, copying said public encryption key from said access card to said source device;

at said source device, (a) encrypting at least some of said digital information in said digital memory using at least one content encryption key to produce encrypted information, (b) using said public encryption key from said destination device to encrypt said content encryption key to thereby generate at least one encrypted content encryption key, and (c) storing said at least one encrypted content encryption key in

said access card;

connecting said port of said digital memory to said digital information port of said destination device;

placing said access card in said access card port of said destination device a second time;

after said step of placing said access card in said access card port of said destination device a second time, copying said at least one encrypted content encryption key from said access card to said destination device, and decrypting said encrypted content encryption key using the private key; and

at said destination device, receiving said encrypted information from said digital memory, and using said content encryption key to decrypt said encrypted information.

11. A method according to claim 10, further comprising the step of establishing that said access card is not expired.

12. A method according to claim 11, wherein said step of establishing that said access card is not expired is performed by comparing the current time with a timestamp in said User Certificate.

13. An access card, said access card comprising:

a memory having at various times at least first, second, and third states;

authenticating means;

said memory comprising, in said first state, a second Conditional Access Certificate (A) and a first User Certificate (B) stored therein;

said memory, in said second state, following a first insertion of said card and first authentication, where said first insertion of said card is into an access card port of a digital information destination device including (a) a digital information port which is capable of receiving said digital information, (b) a second stored User Certificate (A) and (c) mutually corresponding private and public encryption keys associated with said destination device, and said first authentication is performed by said authenticating means authenticating said second User Certificate (A) from said

destination device with said second Conditional Access Certificate (A), comprising said public encryption key from said destination device;

said memory, in said third state, following (i) a second insertion of said card and second authentication, where said second insertion of said card is into an access card port of a digital information source device including (a) a removable digital memory containing digital information and (b) a further memory containing a first Conditional Access Certificate (B) and at least one content encryption key, and also following (ii) authentication of said first User Certificate (B) stored in said memory of said access card with said first Conditional Access Certificate (B) stored in said source device to establish validity of said access card to said source device, comprising said at least one content encryption key encrypted with said public encryption key.